Al Roundtree, OSB # 232263
FOX ROTHSCHILD LLP
1001 Fourth Avenue, Suite 4400
Seattle, Washington 98154
Telephone: 206.624.3600
Facsimile: 206.389.1708

*Attorneys for Amici Curiae Access Now, Gulf Centre for Human Rights*

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

PORTLAND DIVISION

| | |
|---|---|
| LOUJAIN HATHLOUL ALHATHLOUL,<br><br>Plaintiff,<br><br>v.<br><br>DARKMATTER GROUP, MARC BAIER, RYAN ADAMS, and DANIEL GERICKE,<br><br>Defendants. | Case No. 3:21-cv-01787-IM<br><br>**ACCESS NOW AND GULF CENTRE FOR HUMAN RIGHTS' MOTION TO APPEAR AS AMICI CURIAE AND TO SUBMIT AMICUS BRIEF IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS** |

## LOCAL RULE 7-1 CERTIFICATION

In accordance with LR 7-1(a), the undersigned counsel certifies that counsel for the parties have conferred in good faith regarding the substance of this Motion. Plaintiff does not oppose the Motion. Defendants oppose the Motion.

## CERTIFICATE OF COMPLIANCE

This Motion brief and the following brief of amici curiae comply with the applicable word-count limitation under LR 7-2(b). The Motion contains 1,114 words, including headings, footnotes, and quotations, but excluding the caption, table of contents, table of cases and authorities, signature block, exhibits, and any certificates of counsel. The proposed brief of

amici curiae contains 4,693 words, including headings, footnotes, and quotations, but excluding the caption, table of contents, table of cases and authorities, signature block, exhibits, and any certificates of counsel.

## DISCLOSURE STATEMENT

Amici Curiae Access Now and Gulf Centre for Human Rights make the following disclosures:

1) For non-governmental corporate parties please list all parent corporations: None.

2) For non-governmental corporate parties please list all publicly held companies that hold 10% or more of the party's stock: None.

3) No party's counsel authored this brief in whole or in part; no party or a party's counsel contributed money intended to fund the preparation or submission of this brief.

4) No person other than the amici curiae, their members, or their counsel, contributed money intended to fund the preparation or submission of this brief.

## ACCESS NOW AND GULF CENTRE FOR HUMAN RIGHTS' MOTION TO APPEAR AS *AMICI CURIAE*

"[The] district court has broad discretion in the appointment of amici curiae." *Hoptowit v. Ray*, 682 F.2d 1237, 1260 (9th Cir. 1982), *abrogated on other grounds by Sandin v. Conner*, 515 U.S. 472, 487 (1995). "An amicus brief should normally be allowed when . . . the amicus has unique information or perspective that can help the court beyond the help that the lawyers for the parties are able to provide." *Cmty. Ass'n for Restoration of Env't (CARE) v. DeRuyter Bros. Dairy*, 54 F. Supp. 2d 974, 975 (E.D. Wash. 1999). Amicus briefs are "frequently welcome . . . concerning legal issues that have potential ramifications beyond the parties directly involved or if the amicus has unique information or perspective that can help the court beyond the help that the lawyers for the parties are able to provide."



FOX ROTHSCHILD LLP
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

*N.G.V. Gaming, Ltd. v. Upstream Point Molate, L.L.C.*, 355 F. Supp. 2d 1061, 1067 (N.D. Cal. 2005) (citations and internal quotation marks omitted); *see also Netchoice v. Bonta*, 2023 WL 6131619 (N.D. Ca. 2023) (granting leave for numerous briefs filed by civil society organizations, stating that "the Court appreciates the excellent work of all the amici who filed briefs. Those briefs rounded out the arguments presented by the parties and were useful to the Court in considering the important issues raised in this case.").

Amici curiae Access Now and Gulf Centre for Human Rights ("GCHR") are international non-governmental organizations that advocate for and endeavor to protect fundamental human rights and rule of law. Amici are co-leaders of the Middle East and North Africa ("MENA") Surveillance Coalition, which engages in advocacy and strategic litigation with the objectives of ending sales of digital surveillance tools to repressive governments in the region, fighting for a safe and open internet, defending human rights, and protecting human rights defenders, journalists, and internet users from surveillance.

Amici are in a unique position to provide information and expertise on the reasonableness of exercising jurisdiction in this case, as well as the unavailability of meaningful alternative forums or remedies. Amici for years have monitored how mercenary spyware devastates the work of human rights defenders, journalists, and dissidents. As a result, Access Now was permitted to intervene before the Ninth Circuit in ongoing litigation by WhatsApp, Inc. against NSO Group, a competitor of Defendant DarkMatter Group ("DarkMatter"), to provide expertise on the global private surveillance industry and its impact on human rights defenders.[1]

[1] Brief of Access Now, et al. as Amici Curiae in Support of Appellees' Request for Affirmance, *NSO Grp. Techs. Ltd. v. Whatsapp, Inc.*, No. 20-16408 (9th Cir. 2020).



**FOX ROTHSCHILD LLP**
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

Amici have followed the activities of DarkMatter in furthering severe repression by the government of the United Arab Emirates ("UAE"). Amicus GCHR's own advisory board member and prominent Emirati human rights activist Ahmed Mansoor was targeted by mercenary spyware, including that of DarkMatter. ECF No. 54, ¶ 83. This led to his ongoing arbitrary detention and solitary confinement, in which he has been denied a bed, mattress, and pillow, as well as access to adequate medical care, exercise, and sunshine, treatment that UN human rights experts have warned violate basic human rights standards and may constitute torture.[2] There is presently no free human rights defender or independent journalist in the UAE, as all are behind bars or in exile. Mercenary spyware has been instrumental to this extreme level of repression, which has drawn global scrutiny.[3] Amici hope to lend their expertise as the Court conducts an inquiry into the reasonableness and notions of justice in exercising jurisdiction over Defendants.

As set forth in detail in the following amicus brief, the legal issues raised in this case are of immense public interest because they impact the rights of human rights activists, dissidents, and journalists both in the United States and around the world. The deployment of mercenary spyware against civil society actors through Apple, Inc.'s infrastructure, made world news in just recent weeks alone, where over a billion users were impacted by security

[2] United Nations Office of the High Commissioner for Human Rights, UAE: UN experts condemn conditions of detention for jailed activist Ahmed Mansoor (May 7, 2019), https://www.ohchr.org/en/press-releases/2019/05/uae-un-experts-condemn-conditions-detention-jailed-activist-ahmed-mansoor; Amnesty International, United Arab Emirates: Human Rights Defender Ahmed Mansoor Remains Held in Solitary Confinement Five and Half Years On (September 30, 2022), https://www.amnesty.org/en/documents/mde25/6071/2022/en/.

[3] *See infra* notes 19-23 (exploring in depth international attention).



**FOX ROTHSCHILD LLP**
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

vulnerabilities.[4] The problem of mercenary spyware has been named by both the executive[5] and legislative[6] branches, and the Supreme Court declined to halt litigation against a key competitor to DarkMatter. *WhatsApp Inc. v. NSO Grp. Techs. Ltd.*, 17 F.4th 930 (9th Cir. 2021), *cert. denied* 143 S. Ct. 562 (Jan. 9, 2023).

Amici believe their brief will be helpful to the Court in deciding Defendants' Motion because of the nature of the factors-based analysis in determining reasonableness. *Freestream Aircraft (Bermuda) Ltd. v. Aero L. Grp*., 905 F.3d 597, 603–04 (9th Cir. 2018). Specifically, numerous factors including efficient judicial resolution, existence of alternate forums, and the forum state's interest in adjudicating the dispute, are areas in which amici possess significant experience. The parties have briefed the specific facts and law of the

[4] On September 15 and 22, Apple issued emergency updates to over a billion of its users around the world in response to security vulnerabilities exploited by mercenary spyware called 'Pegasus' and 'Predator.' Citizen Lab at the Munk School of Global Affairs at the University of Toronto (Citizen Lab), BLASTPASS: NSO Group iPhone Zero-Click, Zero-Day Exploit Captured in the Wild (Sept. 7, 2023), https://citizenlab.ca/2023/09/blastpass-nso-group-iphone-zero-click-zero-day-exploit-captured-in-the-wild/; Citizen Lab, "Predator in the Wires" (Sept. 22, 2023), https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/. Pegasus, for instance, was discovered on the devices of a civil society member in Washington D.C. Davey Winder, *New Critical Security Warning For iPhone, iPad, Watch, Mac—Attacks Underway*, Forbes (Sept. 21, 2023), https://www.forbes.com/sites/daveywinder/2023/09/21/ios-1701-critical-security-update-warning-for-all-iphone-users/; Lorenzo Franceschi-Bicchierai, *Apple fixes zero-day bugs used to plant Pegasus spyware*, TechCrunch (Sept. 7, 2023), https://techcrunch.com/2023/09/07/apple-fixes-zero-day-bugs-used-to-plant-pegasus-spyware.

[5] The recent order was titled "Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security." Exec. Order No. 14,093, 88 C.F.R. 1895 (2023) (naming a "fundamental" interest in countering the proliferation of commercial spyware misused against activists, dissidents, and journalists).

[6] James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, 136 Stat. 2395; *see* Chris Baumohl et al., *Privacy, Surveillance, and AI in the FY'23 National Defense Authorization Act (NDAA)*, EPIC (Jan. 26, 2023), https://epic.org/privacy-surveillance-and-ai-in-the-fy23-national-defense-authorization-act-ndaa/ (noting how DarkMatter's "Project Raven" led to restrictions on post-intelligence community employment in the 2022 Consolidated Appropriations Act).



FOX ROTHSCHILD LLP
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

matter at hand, and as such amici hope to lend context as to relevant issues in the Gulf region.

Accordingly, amici curiae Access Now and GCHR respectfully request the opportunity to be heard. Amici further request the opportunity to submit a succinct reply to respond to any arguments or analysis that Defendants might submit in response or opposition to the following brief of amici curiae.

Dated: September 26, 2023.

**FOX ROTHSCHILD LLP**

*s/ Al Roundtree*

Al Roundtree, OSB # 232263
1001 Fourth Avenue, Suite 4400
Seattle, Washington 98154
Telephone: 206.624.3600
Facsimile: 206.389.1708
Email: aroundtree@foxrothschild.com

*Attorneys for Amici Curiae Access Now, Gulf Centre for Human Rights*

**BRIEF OF *AMICI CURIAE* ACCESS NOW AND GULF CENTRE FOR HUMAN RIGHTS IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS**

**TABLE OF CONTENTS**





FOX ROTHSCHILD LLP
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

# TABLE OF AUTHORITIES

## FEDERAL CASES AND BRIEFS



## STATUTES



## EXECUTIVE ORDERS



## OTHER AUTHORITIES





FOX ROTHSCHILD LLP
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

**FOX ROTHSCHILD LLP**
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

**FOX ROTHSCHILD LLP**
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

**FOX ROTHSCHILD LLP**
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

**FOX ROTHSCHILD LLP**
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

**FOX ROTHSCHILD LLP**
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

FOX ROTHSCHILD LLP
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

**BRIEF OF *AMICI CURIAE* ACCESS NOW AND GULF CENTRE FOR HUMAN RIGHTS IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS**

## I. IDENTITY AND INTEREST OF *AMICI CURIAE*

**Access Now** has offices in the United States and multiple countries, working to defend and extend the digital rights of people and communities at risk around the world, with particular focus on privacy and data protection, freedom of expression and assembly, digital security, and inclusive connectivity. It began as an emergency response team of technologists working to help people get back online and ensure safe communications after the Iranian government blocked internet access and censored content during the 2009 Iranian election. Access Now has grown to be an organization with international reach, with team members across more than twenty-five countries. Access Now works to hold governments and companies accountable for human rights violations, in courts around the globe.

Access Now has, for instance, analyzed mass surveillance in Syria,[7] supported research on the hacking of Bahraini activists,[8] and monitored surveillance of women human rights defenders in Bahrain and Jordan.[9] Access Now also, jointly with the Citizen Lab at the Munk School of Global Affairs at the University of Toronto (the "Citizen Lab"), investigated El Salvador's use of surveillance software, prompting the Inter-American Commission on Human Rights to express extreme concern over the trend.[10]

---

[7] Access Now, Digital dominion: new report exposes the depth of Syrian regime's mass surveillance (Mar. 18, 2021, updated Jan. 26, 2023), https://www.accessnow.org/press-release/digital-dominion-syrian-regime-mass-surveillance/.
[8] Access Now, Bahraini government hacks activists with NSO Group technology (Aug. 24, 2021, updated Jan. 26, 2023), https://www.accessnow.org/press-release/bahraini-nso-hack/.
[9] Access Now, Unsafe anywhere: women human rights defenders speak out about Pegasus attacks (Jan. 17, 2022, updated May 8, 2023), https://www.accessnow.org/women-human-rights-defenders-pegasus-attacks-bahrain-jordan/.
[10] Access Now, Exposed: civil society condemns use of Pegasus in El Salvador to spy on journalists and activists (Jan. 13, 2022, updated Jan. 26, 2023),



FOX ROTHSCHILD LLP
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

**GCHR**, based in Lebanon, provides support and protection for human rights defenders, including by monitoring the human rights environment in the Gulf Region. Its activities include active protection of the safety of human rights defenders, journalists, and activists both online and offline, as well as raising awareness of and advocating for the defense of human rights regionally. GCHR has worked with and advocated for scores of human rights defenders and journalists who have been targets of spyware exploits by private companies and governments in the Gulf and MENA region, including in Bahrain,[11] Morocco,[12] Jordan,[13] and the UAE,[14] among many countries, as well as with journalists working abroad exposing human rights abuses in the Gulf.

## II. INTRODUCTION

A *New York Times* investigation concluded that DarkMatter "exemplif[ies] the proliferation of privatized spying."[15] Indeed, DarkMatter has been dubbed the "archetype" for

---

https://www.accessnow.org/press-release/pegasus-el-salvador-spyware-targets-journalists-statement/; IACHR Press Office, Press Release, IACHR, Its Special Rapporteurship for Freedom of Expression and OHCHR Are Concerned About Evidence of the Use of Pegasus Malware to Spy on Journalists and Civil Society Organizations in El Salvador (Jan. 31, 2022), https://www.oas.org/en/iachr/jsForm/?File=/en/iachr/media_center/preleases/2022/022.asp.

[11] Gulf Centre for Human Rights, Surveillance of Bahraini human rights defenders, journalists and activists spurs urgent need for action (Aug. 25, 2021), https://www.gc4hr.org/surveillance-of-bahraini-human-rights-defenders-journalists-and-activists-spurs-urgent-need-for-action/.

[12] Gulf Centre for Human Rights, Morocco, "The Kingdom of Terror": The "tactical weapons" used by the Moroccan deep state to stifle dissent (Feb. 23, 2023), https://www.gc4hr.org/morocco-the-kingdom-of-terror/.

[13] Gulf Centre for Human Rights, Protest against Custody Laws, Pegasus targets journalists & Adnan Al-Rousan released (Oct. 25, 2022), https://www.gc4hr.org/protest-against-custody-laws-pegasus-targets-journalists-release-of-adnan-al-rousan/.

[14] Gulf Centre for Human Rights et al., Joint Submission on the United Arab Emirates to the 74th Session of the UN Committee Against Torture (June 26, 2020, updated June 13, 2022), https://www.gc4hr.org/wp-content/uploads/2023/05/UAE-Joint-NGO-submission-to-CAT-Updated-10-June-2022-ENGLISH-final.pdf.

[15] Mark Mazzetti, et al., *A New Age of Warfare, How Internet Mercenaries Do Battle for Authoritarian Governments*, New York Times (Mar. 21, 2019), https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.html.



FOX ROTHSCHILD LLP
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

repression of human rights defenders in the UAE.[16] Several U.S. lawmakers have called for sanctioning DarkMatter for being "complicit in human rights abuses" for hacking into the "devices and accounts of human rights activists and journalists, including Americans, on behalf of the United Arab Emirates."[17] The company has been instrumental to the "cyber-surveillance campaigns" of the UAE government.[18] That has included spying on UAE dissidents,[19] including the imprisoned UAE human rights activist Ahmed Mansoor of GCHR,[20] as well as journalists.[21]

These accounts are consistent with the UAE's dismal human rights record. As amicus GCHR has reported, at least sixty Emirati human rights defenders and dissidents have been

[16] *The hacking industry faces an end of an era*, MIT Technology Review (June 27, 2022), https://www.technologyreview.com/2022/06/27/1054884/the-hacking-industry-faces-the-end-of-an-era/.
[17] Letter from U.S. Lawmakers to Treasury Secretary Janet Yellen and Secretary of State Anthony Blinken (Dec. 15, 2021), https://www.wyden.senate.gov/imo/media/doc/Magnitsky%20Letter%20to%20Sec.%20Yellen%20&%20Blinken.pdf. Signatories also included several U.S. Senators including Ron Wyden, Edward Markey, and Christopher Murphy.
[18] Gulf Centre for Human Rights and International Human Rights Law Clinic at the University of California, Berkeley, School of Law, Who will be Left to Defend Human Rights? Persecution of Online Expression in the Gulf and Neighbouring Countries (Nov. 9, 2021), https://www.gc4hr.org/wp-content/uploads/2023/02/BerkeleyLaw_DigitalRightsReport-1.pdf.
[19] Citizen Lab, "Keep Calm and (Don't) Enable Macros" (May 29, 2016), https://citizenlab.ca/2016/05/stealth-falcon/.
[20] Mr. Mansoor was targeted by multiple spyware firms, including NSO Group, the creator of Pegasus. Citizen Lab, "The Million Dollar Dissident NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender" (August 24, 2016), https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/; Christopher Bing and Joel Schectman, *Inside the UAE's Secret Hacking Team of American Mercenaries*, Reuters (Jan. 30, 2019), https://www.reuters.com/investigates/special-report/usa-spying-raven/.
[21] Committee to Protect Journalists, CPJ Concerned by Report that UAE 'Project Raven' Surveilled Journalists (Jan. 30, 2019), https://cpj.org/mideast/uae/page/2/.



FOX ROTHSCHILD LLP
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

detained for more than ten years, often well past their sentences.[22] The U.S. State Department's most recent review of the UAE highlighted "credible reports" of "serious" and "significant human rights issues" ranging from arbitrary arrest, incommunicado detention, and "transnational repression," to serious restrictions on freedom of speech, privacy, and internet freedom.[23] The UAE has faced similar scrutiny from United Nations mechanisms, human rights NGOs, and peer review from other countries, which has found the UAE engaged in "systematic violations of international due process" in the form of denying adequate access to legal counsel, forced confessions, indefinite detentions, unjust imprisonment, torture, and mistreatment of prisoners.[24]

Against this backdrop, is it reasonable to tell Ms. Alhathloul that her only recourse is the UAE—the very country that persecuted her? Conferring personal jurisdiction over Defendants is consistent with notions of justice and necessary to uphold the rule of law for several specific reasons.

First, DarkMatter's deployment of spyware is part of an ongoing, repressive apparatus that exploits digital infrastructure and services in the United States at the behest of the UAE

[22] Gulf Centre for Human Rights, Joint Statement: UAE Human Rights Record Ahead of COP28 (May 1, 2023), https://www.gc4hr.org/joint-statement-uae-human-rights-record-ahead-of-cop28/.
[23] U.S. Department of State, 2022 Country Reports on Human Rights Practices: United Arab Emirates, https://www.state.gov/reports/2022-country-reports-on-human-rights-practices/united-arab-emirates/.
[24] United Nations Office of the High Commissioner for Human Rights, UAE: UN experts condemn trial of foreign nationals based on forced confessions and call for their release (Feb. 15, 2016), https://www.ohchr.org/en/press-releases/2016/02/uae-un-experts-condemn-trial-foreign-nationals-based-forced-confessions-and; Freedom House, Freedom in the World 2023: United Arab Emirates, https://freedomhouse.org/country/united-arab-emirates/freedom-world/2023; Joint Statement, *supra* note 22.



FOX ROTHSCHILD LLP
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

government and others regionally. The objective of that apparatus is to silence dissidents, stifle investigative journalism, and devastate the work of civil society organizations.

Second, no meaningful judicial relief is possible in the UAE. The UAE ensures a well-established lack of judicial independence and basic deficiencies in the rule of law. This has been acknowledged just in recent months before the United Nations peer review of the UAE.[25]

Third, holding a private mercenary company accountable is consistent with U.S. government efforts, now across several agencies, to curb the use of private spyware and cyber mercenaries against human rights defenders and U.S. national security interests.[26] It is also consistent with UN and global priorities, as well as the objectives of coalitions which the United States itself has spearheaded.[27]

## III. ARGUMENT

The rights most directly threatened by surveillance technology like DarkMatter's are the rights to freedom of expression and privacy, which are inextricably bound and which

[25] Human Rights Council, Report of the Working Group on the Universal Periodic Review, United Arab Emirates, U.N. Doc. A/HRC/54/15 (June 29, 2023), Recommendations 35.136-38, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G23/125/41/PDF/G2312541.pdf?OpenElement. As part of the UAE's review, several countries highlighted severe obstacles to obtaining judicial relief, that impacted the "right to complain and resort to justice"; New Zealand stressed the need to "ensure independence of the judiciary from the executive branch." *Id.*

[26] Press Release, Bureau of Industry and Security (July 18, 2023), https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3297-2023-07-18-bis-press-package-spyware-document/file; Exec. Order, *supra* note 5.

[27] *See, e.g.*, Human Rights Council, Report of the Office of the United Nations High Commissioner for Human Rights, U.N. Doc. A/HRC/51/17 (Aug. 4, 2022), ¶¶ 6-19, https://undocs.org/A/HRC/51/17 (discussing escalating international scrutiny and concern over mercenary spyware such as Pegasus); Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware, White House (Mar. 30, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/30/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/.



FOX ROTHSCHILD LLP
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

international law recognizes as foundational.[28] These are enshrined in instruments such as the International Covenant on Civil and Political Rights ("ICCPR"), and the Universal Declaration of Human Rights. In furtherance of the protection of these rights—and against the backdrop of malicious actors like DarkMatter targeting Apple security infrastructure in the United States in order to undermine those rights at the behest of the UAE and other regimes in the Middle East—exercising jurisdiction over Defendants in this matter is reasonable.

### A. DarkMatter's Clandestine Targeting of Secure Devices and Services Is a Key Instrument in UAE Repression of Human Rights Defenders Across Borders, that the United States Has a Strong Interest in Addressing

Amici have monitored how the mercenary spyware industry, time after time again, has targeted the infrastructure of Apple, Inc. and other U.S. companies to surveil the communications of human rights defenders regionally and worldwide, with the ultimate goal of compromising their work.

#### i. Vulnerable Groups Rely on the U.S.-Based Security Infrastructure of Apple Devices and Services for Their Safety

Like most of us, human rights defenders rely on the security infrastructure of Apple's devices and services, which makes them target for sophisticated spyware.[29] Specifically, iPhones are utilized by many human rights defenders due to their reputation for enhanced security features, including their utilization of U.S.-based servers, safeguards, and technology which have a reputation for safety, in line with Apple's marketing of its products and services

[28] Electronic Frontier Foundation, International Principles on the Application of Human Rights to Communications Surveillance (May 2014), https://www.eff.org/files/necessaryandproportionatefinal.pdf.

[29] Brief of Access Now, et al. *supra* note 1 at 7 (noting that human rights defenders and similar actors "choose encrypted technologies like WhatsApp to prevent [abusive] governments from intercepting communications and conducting intrusive surveillance"); John Naughton, *The WhatsApp spyware story tells us that nothing is secure*, The Guardian (May 19, 2019), https://www.theguardian.com/commentisfree/2019/may/19/whatsapp-spyware-story-tells-us-nothing-is-secure-pegasus-nso.



FOX ROTHSCHILD LLP
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

as privacy-protecting. ECF No. 54, ¶ 152. For this reason, users trust Apple with storing notifications, data, and message attachments on their servers in the United States. *Id.* ¶¶ 114-16. This confidence also makes Apple devices a ripe target for actors that have an interest in accessing protected information and communications. The compromise of secure platforms can have devastating consequences.

ii. The UAE and Neighboring Countries Use Spyware to Dismantle Human Rights Networks Across Borders

Commercial spyware has important transnational implications across all fifty U.S. states, as digital surveillance makes it easier for regimes to monitor their targets across borders. Citizen Lab has found that cross-border surveillance is "a relatively common practice."[30] There is presently no free human rights defender or independent journalist in the UAE, as all are behind bars or in exile, making spyware an essential tool for the UAE to expand its repression beyond its borders. Indeed, mercenary spyware companies have actively sought lucrative business deals with the governments in the Gulf region, leading to the proliferation of spyware use across several Gulf states, including the UAE.[31] The ubiquitous spread of commercial

[30] Citizen Lab, "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries" (2018), at 25, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/ (finding how "[t]en Pegasus operators appear to be conducting surveillance in multiple countries. While we have observed prior cases of cross-border targeting, this investigation suggests that cross-border targeting and/or monitoring is a relatively common practice."). Since there are no free human rights defenders or independent journalists in the UAE–they are either behind bars or are in exile–spyware is an essential tool for the government to expand its repression beyond its borders.

[31] Chaim Levinson, *With Israel's Encouragement, NSO Sold Spyware to UAE and Other Gulf States*, Haaretz (Aug. 25, 2020), https://www.haaretz.com/middle-east-news/2020-08-25/ty-article/.premium/with-israels-encouragement-nso-sold-spyware-to-uae-and-other-gulf-states/0000017f-dbf3-d856-a37f-fff3a4ba0000.



FOX ROTHSCHILD LLP
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

spyware led hundreds of civil society organizations and individuals worldwide to highlight the detrimental impact that the technology has on human rights.[32]

As GCHR has closely monitored for years, the regional and global nature of surveillance is of particular concern given widespread internet control and surveillance in the Gulf region, particularly of human rights defenders. Based on recent revelations, Bahrain, Oman, Qatar, Saudi Arabia, and UAE surveil or gain access to private communications of human rights activists targeted for their online activism.[33] For instance, the Citizen Lab found evidence of spyware on mobile phones in Bahrain, Oman, and Saudi Arabia, in addition to the UAE, which would have allowed those governments to monitor the infected individuals' private communications.[34] Indeed, researchers have confirmed how DarkMatter's use extends well beyond the UAE.[35]

Governments seek not only to silence individual targets, but strike fear into and undermine entire movements that span borders. In a profile of five MENA countries, one

---

[32] Gulf Centre for Human Rights, Civil society organisations address a joint statement to states participating in the Summit for Democracy 2023 (Mar. 28, 2023), https://www.gc4hr.org/civil-society-organisations-address-a-joint-statement-to-states-participating-in-the-summit-for-democracy-2023-states-investors-have-a-responsibility-to-curtail-the-abuse-of-spyware/; Access Now, Geneva Declaration: international community unites to end spyware abuse (Sep. 29, 2022), https://www.accessnow.org/press-release/geneva-declaration-end-spyware-abuse/; Amnesty International, Joint open letter by civil society organizations and independent experts calling on states to implement an immediate moratorium on the sale, transfer and use of surveillance technology (Jul. 27, 2021), https://www.amnesty.org/en/documents/doc10/4516/2021/en/.

[33] Levinson, *supra* note 31.

[34] Who will be Left to Defend Human Rights, *supra* note 18 (documenting 225 incidents between May 2018 and October 2020); Citizen Lab, "Pearl 2 Pegasus" (Feb. 18, 2022), https://citizenlab.ca/2022/02/bahraini-activists-hacked-with-pegasus/.

[35] *See* Shaheed Ahmed and Greenacre Benjamin "Binary Threat: How Governments' Cyber Laws and Practice Undermine Human Rights in the MENA Region," *POMEPS*, Studies 43: Digital Activism and Authoritarian Adaptation in the Middle East (Aug. 2021), https://pomeps.org/the-web-insecurity-of-mena-civil-society-and-media (detailing reach to Saudi Arabia, Egypt, Morocco, Algeria, and Sudan among others).



FOX ROTHSCHILD LLP
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

researcher found that "each country used spyware in concert with different forms of physical and digital repression."[36] This trend has prompted grave concern from the international community. The Council of Europe recognizes the "chilling effect" that spyware has on the exercise of fundamental rights generally, including the right to dignity, freedom of assembly, freedom of religion, and even the physical and psychological integrity of individuals.[37] The United Nations and its Special Procedures have maintained a clear consensus calling for a moratorium on the trade and use of mercenary spyware. The UN High Commissioner for Human Rights has warned of the "growing landscape of spyware marketed by companies to Governments across the globe."[38] Regionally, the Inter-American Commission on Human Rights has echoed the calls for a moratorium, expressing deep concern over the deployment of mercenary spyware.[39] And the European Parliament, as well, recently adopted a resolution asserting that mercenary spyware puts "democracy itself at stake."[40]

It is against this backdrop that DarkMatter's hacking of Ms. Alhathloul was part of a broader effort by the UAE and Saudi Arabia to devastate the women's rights movement. Human Rights Watch recently submitted to the United Nations a finding in Saudi Arabia that "[t]he arrests, torture and travel bans against women's rights activists has had a chilling effect

---

[36] Gail Horak, Master's Thesis, "Personal Details Exposed: Spyware and Human Rights in the Middle East and North Africa," Harvard University Division of Continuing Education (2023), at 137, https://nrs.harvard.edu/URN-3:HUL.INSTREPOS:37374983.
[37] Tamar Kaldani and Zeev Prokopets, Pegasus Spyware and its impacts on human rights, Council of Europe Information Society Department (June 20, 2022), at 5, https://rm.coe.int/pegasus-spyware-report-en/1680a6f5d8.
[38] *Supra* note 27.
[39] IACHR Press Office, *supra* note 10.
[40] Press Release, European Parliament, Spyware: MEPs call for full investigations and safeguards to prevent abuse (June 15, 2023), https://www.europarl.europa.eu/news/en/press-room/20230609IPR96217/spyware-meps-call-for-full-investigations-and-safeguards-to-prevent-abuse.



FOX ROTHSCHILD LLP
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

that has prevented women from speaking out."[41] And Costa Rica called on the UAE to issue a "moratorium on the use of spyware technology and introduce human rights-based monitoring mechanisms."[42]

iii. Zero-Click, Zero-Day Exploits, Like the One Used by DarkMatter's Spyware, Are the "Holy Grail" for Repressive Regimes

DarkMatter, beginning in or about late 2015 or early 2016, operated a cyber-surveillance program dubbed Project Raven. ECF No. 54, ¶ 6. DarkMatter, for its use of Project Raven, has faced scrutiny for targeting governments, dissidents, and human rights defenders in the UAE and in the broader Middle East.[43] DarkMatter developed and repeatedly deployed spyware known as "Karma," which used a "zero-click," "zero-day" iMessage exploit. ECF No. 54, ¶ 92. This exploit leveraged a vulnerability in the Apple iMessage app to install spyware on the target's iPhone and exfiltrate data. *Id.* Zero-click exploits—which do not require any action from the victim—are rare. They are "especially prized by attackers" and are considered the "holy grail" of exploits as they do not require any actions by the victim to be installed on the device.[44] "Zero-day," on the other hand, refers to a vulnerability being unknown until

[41] Human Rights Watch, Submission to the Universal Periodic Review of Saudi Arabia (July 2023), at 7, https://www.hrw.org/sites/default/files/media_2023/07/Human%20Rights%20Watch%20Submission%20to%20the%20Universal%20Periodic%20Review%20of%20the%20Kingdom%20of%20Saudi%20Arabia_0.pdf.

[42] Report of the Working Group on the Universal Periodic Review, United Arab Emirates, *supra* note 25, Recommendation 35.166.

[43] Jenna McLaughlin, *How the UAE is recruiting hackers to create the perfect surveillance state*, The Intercept (Oct. 24, 2016), https://theintercept.com/2016/10/24/darkmatter-united-arab-emirates-spies-for-hire/.

[44] *Id.*; Mike Fong, *The Pernicious Invisibility Of Zero-Click Mobile Attacks*, Forbes (Dec. 14, 2020), https://www.forbes.com/sites/forbestechcouncil/2020/12/14/the-pernicious-invisibility-of-zero-click-mobile-attacks/.



FOX ROTHSCHILD LLP
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

disclosure to the company.[45] Zero-day exploits are inherently dangerous for the security of mobile devices, as they are vulnerabilities that manufacturers are unaware of until someone discloses them.[46]

iv. Mercenary Spyware Companies in the UAE, Like DarkMatter, Actively Seek to Avoid Detection and Accountability

Mercenary spyware firms have a strong incentive to cover their tracks in exploiting vulnerabilities. Following the discovery and disclosure of the aforementioned iPhone vulnerabilities in September, Apple patched the exploits within days.[47] Evading detection preserves the value of the exploit to the attacker, and therefore maximizes the damage caused. For this reason, undiscovered exploits are worth enormous sums of money on black markets, at times in the millions.[48] Hence, evading detection is a key priority for mercenary spyware companies.[49]

Defendants masked the origin of their hacking transmissions including by routing their communications through U.S.-based anonymization services and other proxy servers hosted in the United States to prevent detection and attribution. ECF No. 54, ¶¶ 107-08. In doing so, like NSO and other firms specifically targeting devices and platforms, DarkMatter could avoid

---

[45] Evan Hill and Joseph Menn, *Egyptian presidential hopeful targeted by Predator spyware*, Washington Post (Sept. 23, 2023), https://www.washingtonpost.com/investigations/2023/09/23/predator-egypt-hack-spyware-iphone/.

[46] *Id.*

[47] *See supra* note 4 (discussing Apple's patching of vulnerabilities).

[48] Andy Greenberg, *Why 'Zero Day' Android Hacking Now Costs More Than iOS Attacks*, Wired (Sept. 3, 2019), https://www.wired.com/story/android-zero-day-more-than-ios-zerodium/.

[49] Consider the now-defunct firm FinFisher, which did not even deploy the most-prized zero-click attacks. Access Now, Surveillance Tech For Sale—Alert, FinFisher Changes Tactics to Hook Critics (May 2018), https://www.accessnow.org/wp-content/uploads/2018/05/FinFisher-changes-tactics-to-hook-critics-AN.pdf.



FOX ROTHSCHILD LLP
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

detection and preserve the immense value of a compromise that would otherwise be worthless once discovered.

### B. Alternative Relief Is Impossible for Ms. Alhathloul, as the UAE Suffers from a Well-Established Lack of Basic Judicial Safeguards

There is no meaningful possibility of judicial relief for the many human rights defenders impacted by commercial spyware in the UAE, or Gulf Region generally. The U.S. State Department in its 2022 Human Rights Country Report on the UAE observed that the country's "[c]ourts lacked full independence."[50] Plaintiffs and their attorneys frequently face harassment or threats where cases implicate the government, and human rights attorneys serve prison time for their work. Further, ongoing discrimination against women in law and practice only complicates access of women like Ms. Alhathloul to the legal system.[51] Further, these are the very countries that persecuted her.

These judicial deficiencies are plainly echoed by others at the international level. The UAE just completed its Universal Periodic Review, a mechanism through the UN Human Rights Council where UN Member States undergo a 'peer review' of their human rights records every 4.5 years. As part of UAE's review, several countries highlighted severe obstacles to obtaining judicial relief that impacted the "right to complain and resort to justice;" New Zealand stressed the need to "ensure independence of the judiciary from the executive branch."[52]

---

[50] U.S. Department of State, 2022 Country Reports on Human Rights Practices: United Arab Emirates, *supra* note 23.
[51] *See* Human Rights Watch, United Arab Emirates, Events of 2021, https://www.hrw.org/world-report/2022/country-chapters/united-arab-emirates ("While the UAE has made a few reforms, it continues to discriminate against women in [its] law and practice").
[52] *Supra* note 25.



FOX ROTHSCHILD LLP
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

As such, outside of the present litigation, there is no credible way Plaintiff will ever find judicial relief. Indeed, a review of Citizen Lab's analysis of worldwide efforts to obtain judicial relief against spyware companies over the last five years for conduct alleged in the UAE or Gulf countries do not show a single proceeding in those jurisdictions, despite the concentration of mercenary spyware activities in the Gulf.[53]

These concerns with the UAE's judicial system have persisted for years. In 2015, the UN Special Rapporteur on the independence of judges and lawyers issued a report following an official mission to the UAE. The Rapporteur's report noted the lack of independence and transparency in the judiciary, as well as harassment and threats faced by lawyers litigating state security crimes.[54] Amicus GCHR has noted how the detention of human rights lawyer Mohammed Al-Roken violated the UN Basic Principles on the Role of Lawyers.[55]

These deficiencies have been echoed by the UN Special Rapporteur on freedom of opinion and expression, the UN's chief independent expert on matters of freedom of speech online, who issued a comprehensive report studying "case after case of Governments using surveillance software developed, marketed, and supported by private companies."[56] He

---

[53] See Citizen Lab, "Litigation and other formal complaints related to mercenary spyware" (Dec. 12, 2018, updated July 31, 2023), https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/ (analyzing legal efforts against eight spyware companies).

[54] Human Rights Council, Report of the Special Rapporteur on the independence of judges and lawyers, Gabriela Knaul, Addendum, U.N. Doc. A/HRC/29/26/Add.2 (May 5, 2015), ¶¶ 86-87, https://digitallibrary.un.org/record/797649?ln=en.

[55] Gulf Centre for Human Rights, Open letter calling for release of prominent lawyer and human rights defender Dr Mohammed Al-Roken (Nov. 13, 2019), https://www.gc4hr.org/open-letter-calling-for-the-release-of-prominent-lawyer-and-human-rights-defender-dr-mohammed-al-roken/.

[56] Surveillance and human rights, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/HRC/41/35 (May 28, 2019), ¶ 1, https://www.ohchr.org/en/documents/thematic-reports/ahrc4135-surveillance-and-human-rights-report-special-rapporteur.



FOX ROTHSCHILD LLP
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

specifically cited DarkMatter's Project Raven, and commented in response that "[g]overnment regulation . . . with respect to the private surveillance industry appears at best weak and likely does not exist in many, if not most, legal systems."[57] The Rapporteur further highlighted the lack of effective judicial relief in spyware cases, stating that "barriers to successful litigation and formal complaints are significant, including the lack of judicial oversight, remedies, causes of action, enforcement and data preservation."[58]

### C. Jurisdiction Over DarkMatter Is Entirely Consistent With U.S. Priorities to Combat the Mercenary Spyware Epidemic

The United States has a strong interest in adjudicating matters arising from spyware abuses that leverage U.S.-based secure services and platforms. Amicus Access Now has monitored how addressing the problem of spyware use by repressive regimes is consistent with a plethora of recent actions by the executive and legislative branches spearheading a global push to stop the use of commercial spyware in human rights abuses. In March, President Biden signed an Executive Order affirming that the United States has a "fundamental" interest in countering the proliferation of commercial spyware misused against activists, dissidents, and journalists.[59] The United States has hence spearheaded a coalition of allied governments that joined together in stressing how the "powerful and invasive tools" are used to suppress dissent, limit freedom of speech, engage in unlawful surveillance, and otherwise abuse civil rights.[60]

---

[57] *Id.* ¶ 20.
[58] *Id.* ¶ 41.
[59] *Supra note* 5.
[60] Those countries include Australia, Canada, Costa Rica, Denmark, France, New Zealand, Norway, Sweden, Switzerland, the United Kingdom, and the United States. *Supra* note 27.



FOX ROTHSCHILD LLP
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

The State Department affirmed that spyware has "facilitated repression and enabled human rights abuses, including to . . . monitor and target activists and journalists."[61]

In the courts, the Supreme Court this year declined to halt ongoing litigation against DarkMatter competitor NSO Group,[62] for its compromise of the secure messaging of WhatsApp. In allowing the case to proceed, the Court kept in place the Ninth Circuit's rejection of a foreign sovereign immunity challenge where NSO Group, a private company, was alleged to work on behalf of a foreign government. *WhatsApp Inc. v. NSO Grp. Techs. Ltd.*, 17 F.4th 930 (9th Cir. 2021), *cert. denied* 143 S. Ct. 562 (Jan. 9, 2023). Of note is that the United States, intervening as amicus curiae in the petition for *certiorari*, agreed that the Ninth Circuit reached the "correct result."[63] As a private company alleged to act on behalf of a foreign government, "NSO plainly is not entitled to immunity here."[64] While that position was limited to that proceeding, it signals the current posture of the Supreme Court and the executive branch in contemplating relief against private companies responsible for spyware, even where they are alleged to act in furtherance of a repressive government.

Legislatively, Project Raven prompted a New York congressman to call its activities "absolutely chilling" in introducing a law, subsequently passed, requiring U.S. intelligence

---

[61] Press Release, Department of State (July 18, 2023), https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities-2/.

[62] 'Pegasus' was developed by the NSO Group, an Israeli-based mercenary spyware company that governments around the world have been deploying against journalists, human rights defenders, lawyers, opposition politicians, and dissidents around the world since at least 2016. David Pegg, Sam Cutler, *What is Pegasus spyware and how does it hack phones?*, The Guardian (July 18, 2021), https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones.

[63] *NSO Grp. Techs. Ltd. v. WhatsApp, Inc.*, Brief for the United States as Amicus Curiae, On Petition for a Writ of Certiorari to the United States Court of Appeals for the Ninth Circuit, No. 21-1338 at 7 (Nov. 2022), https://www.supremecourt.gov/DocketPDF/21/21-1338/247116/20221121154250394_NSO%20v.%20WhatsAppp%20CVSG.pdf.

[64] *Id.*



FOX ROTHSCHILD LLP
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

agencies to provide annual risk assessments of former employees working for foreign governments.[65] Project Raven also prompted subsequent restrictions on post-intelligence community employment in the 2022 Consolidated Appropriations Act.[66] It also led to a coalition of U.S. lawmakers, including Adam Schiff, Chairman of the House Permanent Select Committee on Intelligence, and Gregory Meeks, Chairman of the House Foreign Affairs Committee, to call for the imposition of sanctions against DarkMatter for being "complicit in human rights abuses enabled through the surveillance technologies and services they sold to their authoritarian foreign government customers."[67]

## IV. CONCLUSION

Mercenary spyware companies who actively attempt to stifle human rights defenders, activists, and journalists in the United States and around the world should not be above the law. DarkMatter's deployment of spyware is part of an ongoing, repressive apparatus that exploits infrastructure and services in the United States at the behest of the UAE government and others regionally. No meaningful judicial relief is possible in the UAE. And, holding mercenary spyware companies accountable where they have availed themselves of U.S. jurisdiction is also consistent with UN and global priorities, as well as the objectives of coalitions of like-minded governments which the United States has spearheaded. For these reasons, amici submit that providing a chance for justice for Ms. Alhathloul by granting jurisdiction is more than

[65] Schectman and Bing, *supra* note 20; National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, 133 Stat. 2174, 2162.
[66] Pub. L. No. 117-263, *supra* note 6; Baumohl et al., *supra* note 6 ("These restrictions came in response to the Project Raven scandal, in which former intelligence agency employees worked for companies linked to the United Arab Emirates (UAE), eventually conducting cyber espionage against human rights activists, journalists, and the UAE's political foes.").
[67] Letter from U.S. Lawmakers to Treasury Secretary Janet Yellen and Secretary of State Anthony Blinken, *supra* note 17.



FOX ROTHSCHILD LLP
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600

reasonable; it is her only meaningful chance for justice. If U.S. actors cannot be held to account in U.S. courts for their actions, which deeply concern U.S. interests, then where can victims ever seek a remedy?

Dated: September 26, 2023.

**FOX ROTHSCHILD LLP**

*s/ Al Roundtree*

Al Roundtree, OSB # 232263
1001 Fourth Avenue, Suite 4400
Seattle, Washington 98154
Telephone: 206.624.3600
Facsimile: 206.389.1708
Email: aroundtree@foxrothschild.com

*Attorneys for Amici Curiae Access Now, Gulf Centre for Human Rights*[68]

[68] Carey Shenkman, also representing *amici curiae*, assisted in the preparation of this brief.

**CERTIFICATE OF SERVICE**

I certify that I am a secretary at the law firm of Fox Rothschild LLP in Seattle, Washington. I am a U.S. citizen over the age of eighteen years and not a party to the within cause. On the date shown below, I caused to be served a true and correct copy of the foregoing on counsel of record for all other parties to this action.

I declare under penalty of perjury under the laws of the State of Washington that the foregoing is true and correct.

EXECUTED September 26, 2023 , in Seattle, Washington.

*/s/ Martha W. Johns*

Martha W. Johns



**FOX ROTHSCHILD LLP**
1001 FOURTH AVENUE, SUITE 4400
SEATTLE, WA 98154
206.624.3600